Q1 Team Name
0 Points

INSYNC

Q2 Commands
10 Points

List the commands used in the game to reach the ciphertext.

go, back, read

Q3 CryptoSystem
10 Points

What cryptosystem was used in this level?

Playfair Cipher

Q4 Analysis
20 Points

What tools and observations were used to figure out the cryptosystem? (Explain in less than 300 words)

After typing the first command 'go', we saw some code made up of dash and dots. This gave us an idea about morse code. After solving the morse code using their letter mappings, the text that we got was "CRYPTANALYSIS". Along with this, the text told us to PLAY FAIR indicating that Playfair Cipher was being used. After typing 'read' on the first screen, we got the ciphertext. As Playfair

uses a grid and a key to construct the grid, we used "CRYPTANALYSIS" as the key to break it using the decryption process of Playfair Cipher. Extra X's were removed to get the final plaintext:
BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE JOY THERE.
SPEAK OUT THE PASSWORD "ABRA_CA_DABRA" TO GO THROUGH. MAY YOU HAVE THE
STRENGTH FOR THE NEXT CHAMBER. TO FIND THE EXIT YOU FIRST WILL NEED TO
UTTER MAGIC WORDS THERE.

Q5 Decryption Algorithm

15 Points

Briefly describe the decryption algorithm used. Also mention the plaintext you deciphered. (Use less than 350 words)

->As we know that Play-fair Cipher is a manual symmetric encryption technique.
->It is multiple letter encryption cipher that uses 5*5 matrix(which is constructed using special keyword known as key, which in our case was "CRYPTANALYSIS".)

#Step-1 : We generated 5*5 matrix using keyword(repeated letters in keyword are written only once in matrix{ex: A,S}):
->['C', 'R', 'Y', 'P', 'T']
->['A', 'N', 'L', 'S', 'I/J']
->['B' ,'D', 'E', 'F', 'G']
->['H', 'K', 'M', 'O', 'Q']
->['U', 'V', 'W', 'X', 'Z']

#Step-2 : Using the standard rules, we started the decryption of cipher. The rules that we used are mentioned below:
(1) Generate Diagrams: Split the cipher into pieces of two letters(DF ULYP XO CQ->DF UL YP XO CQ).

(2)Column rule: If two letters of cipher appears at same column in 5*5 matrix then to get corresponding plain text shift them up by

one column in 5*5 matrix(do wrap around in case of last cell).

(3)Row rule: If two letters of cipher appears at same row in 5*5 matrix then to get corresponding plain text left shift them by one cell in 5*5 matrix(do wrap around in case of last cell).

(4)Rectangle rule : If two letters of cipher appears in different row&column in 5*5 matrix then in order to get corresponding plain text form a rectangle whose dimensions are limited based on cipher text letters positions.
->To get plain text for top element in rectangle : the first element of same row in rectangle will be corresponding plain text.
->To get plain text for bottom element in rectangle : the last element of same row in rectangle will be corresponding plain text.

#Step-3: Decryption using rules mentioned above :
->Cipher text that we got was:
"DF ULYP XO CQD LFWC RUBHEDY, CQDYG LN XDYL EGIYIG LMP CQDYF.
LYFNH HXPZ CQF YNILXKPB "NDCB_AN_BBHCN" PQ FQ CQPKZBK. OLC PMC
UNUG YMB IPYDIDCQ OXY CMB LDZP AULHDFY. CX OALG RMB FWGI PMX
BNTIP ZLSWS LFWFE PQ ZCYGY KIBAT XMNKI PMBYD."

->Decyption done as follows :
(1) 'DF' : Using the 5*5 matrix that we built, we can see that 'DF' appears in same row hence according to row rule, left shift them to get plain text. Hence D->'B',F->'E'

(2)'UL' : Different row and column, so applied the rectangle rule. To get plain text for 'U', go to the last element of same row in that rectangle hence 'U'->W.
To get plain text for 'L', go to the First element of same row in that rectangle hence 'L'->'A'.

(3) 'YP' : used 5*5 matrix that we built, we can see that 'DF' appears in same row.Hence according to row rule, left shift them to get plain text. Hence Y->'R', P->'Y'

->Using similar procedure we decrypted the whole cipher.

#Step-4: After Decryption we got some unnecessary 'X' in plain text which were filler letters embedded in plain text in order to make diagrams (two letter pairs). Hence we can remove the X's to get more comprehensible plain text.

#Step-5: Final plain text is
BE WARY OF THE NEXT CHAMBER, THERE IS VERY LITTLE JOY THERE.
SPEAK OUT THE PASSWORD "ABRA_CA_DABRA" TO GO THROUGH. MAY YOU HAVE THE
STRENGTH FOR THE NEXT CHAMBER. TO FIND THE EXIT YOU FIRST WILL NEED TO
UTTER MAGIC WORDS THERE.

#We used the following References for Playfair Cipher and Morse Code:
(1) Morse Code : https://en.wikipedia.org/wiki/Morse_code#/media/File:International_Morse_Code.svg
(2) Playfair cipher : https://www.youtube.com/watch?v=UURjVI5cw4g
(3) Playfair cipher : https://www.youtube.com/watch?v=whEJfas9MAI
(4) Playfair cipher: https://www.youtube.com/watch?v=hHsUJxikM3g

Q6 Password

10 Points

What was the final command used to clear this level?

ABRA_CA_DABRA

Q7 Code

0 Points

Upload any code that you have used to solve this level

No files uploaded

Assignment 2

GRADED

GROUP

Punit Chaudhari
Piyush Gangle
Aman Mittal

View or edit group

TOTAL POINTS

64.5 / 65 pts

QUESTION 1

Team Name — **0** / 0 pts

QUESTION 2

Commands — **10** / 10 pts

QUESTION 3

CryptoSystem — **10** / 10 pts

QUESTION 4

Analysis — **20** / 20 pts

QUESTION 5

Decryption Algorithm — R **14.5** / 15 pts

QUESTION 6

Password — **10** / 10 pts

QUESTION 7

Code — **0** / 0 pts